UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/652,010	08/29/2003	Art H. Burget	200207300-1	9679

22879 7590 08/06/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
08/06/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/652,010
Filing Date: August 29, 2003
Appellant(s): BURGET ET AL.

Steven L. Nichols
Reg. No. 40,326
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 23 April 2009 appealing from the Final Office action mailed 18 September 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: Claims 13-18, 30-38 and 40-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Slick et al U.S. Patent No. 7,305,556 B2.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,305,556	Slick et al	12-2007
2002/0169002	Imbrie et al	11-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 13-18, 30-38 and 40-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Slick et al U.S. Patent No. 7,305,556 B2.

As to claim 13, Slick et al discloses a method of controlling a user's ability to cause a client to send a print job to a printer [column 6, lines 37-49]. Slick et al discloses the method comprising providing the client with a key specifically configured for the user [column 6, lines 37-49], wherein the client will refuse to submit a print job to the printer for a particular user unless the key associated with that user has been provided to the client [column 12, lines 1-23].

As to claim 14, Slick et al discloses the method further comprising:

generating the key with a print server [column 6 line 50 to column 7 line 4]; and

transmitting the key to the client from the print server over a network to which the print server, client and printer are all connected [column 6 line 50 to column 7 line 4].

As to claim 15, Slick et al discloses the method further comprising:

storing a related key on a storage device of the print server [column 8, lines 9-17].

As to claims 16 and 33, Slick et al discloses the method further comprising:

encrypting the print job with the key resulting in an encrypted print job [column 6, lines 37-49];

sending the encrypted print job from the client to the print server [column 6, lines 37-49]; and

attempting to decrypt the encrypted print job with the related key stored on the storage device of the print server [column 11, lines 36-53];

wherein, if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

As to claims 17 and 35, Slick et al discloses that the key allows the client to print to multiple networked printers managed by the print server [column 6, lines 8-21].

As to claims 18 and 36, Slick et al discloses that the key is provided to multiple clients [column 6 line 50 to column 7 line 4].

As to claim 30, Slick et al discloses a system for controlling a user's ability to cause a client to print a print job to a printer on a network, the system comprising:

a client [column 9, lines 18-47]; and

a print server for managing at least one network printer, wherein the print server provides a key to the client for use in submitting a print job, the key being specific to a particular user of the client [column 9, lines 18-47];

wherein the client will refuse to submit a print job for a user unless the client has been previously provided with a key specific to that user [column 12, lines 1-23].

As to claim 31, Slick et al discloses that the print server comprises:

a configuration utility for configuring the key [column 7, lines 44-61]; and

a storage device for storing a related key[column 7, lines 44-61].

As to claim 32, Slick et al discloses that the print server:

configures the key specifically for the user with the configuration utility [column 7, lines 44-61];

stores a related key on the storage device [column 7, lines 44-61];

associates the key with a printer driver for the printer [column 7, lines 44-61]; and

installs the key in association with the driver on the client [column 7, lines 44-61].

As to claim 34, Slick et al discloses that if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

As to claim 37, Slick et al discloses that the configuration utility is an embedded web server that resides on the print server [column 9, lines 18-47].

As to claim 38, Slick et al discloses a system controlling use of a printer on a network, the system comprising:

a client connected to the network for generating a print job for the printer [column 9, lines 18-47];

means for providing a key to the client, wherein the key is specific to a user of the client and is used to encrypt a print job from the client to the printer [column 9, lines 18-47]; and

means on the client for encrypting the print job using the key to produce an encrypted print job for transmission to the printer.

As to claim 40, Slick et al discloses decryption means for using a related key to decrypt the print job for use by the printer [column 11, lines 36-53].

As to claim 41, Slick et al discloses that the decryption means comprise a printer server [column 11, lines 36-53].

As to claim 42, Slick et al discloses that the key is used by multiple clients on the network [column 6, lines 8-21].

As to claim 43, Slick et al discloses that the client is configured to use the key to submit the print job only at the request of the particular user [column 7, lines 44-61].

As to claim 44, Slick et al discloses that the means for providing a key comprise a print server on the network [column 6, lines 8-21].

As to claim 45, Slick et al discloses that the printer server further comprises:

means for storing a related key on a storage device of the print server [column 9, lines 18-47];

means for associating the key with a printer driver for the printer [column 9, lines 18-47]; and

means for installing the key in association with the printer driver on the client [column 9, lines 18-47].

As to claim 46, Slick et al discloses that the printer server further comprises:

means for attempting to decrypt the encrypted print job with a related key [column 11, lines 36-53];

wherein, if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-10 and 19-29 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick et al U.S. Patent No. 7,305,556 B2 in view of Imbrie et al US 2002/0169002 A1.

As to claim 1, Slick et al discloses a method of controlling use of a printer on a network, the method comprising:

with a print server, generating a key for a specific client of the print server;

wherein the key is used to submit a print job from the client to a printer on the network [column 6, lines 37-49].

Slick et al does not teach embedding the key in a printer driver. Slick et al does not teach providing the key to the specific client on the network by installing the print driver on the specific client.

Imbrie et al teaches permitting encryption/decryption of data received from the intermediate device, a public key can be provided and embedded within the print driver for use with a later generated private key to encrypt or decrypt data pockets transmitted from the printing assembly 40 [0037].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Slick et al so that the key pair would have been embedded in a print driver and the keys would have been provided to the client when the driver was installed on the specific client.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Slick et al by the teaching of Imbrie et al because it provides a secure manner in which keys are distributed with differing peripheral devices [0007].

As to claim 2, Slick et al teaches using the key to encrypt the print job on the client prior to transmission of the print job to the printer [column 6, lines 37-49].

As to claim 3, Slick et al teaches using the key or a related key to decrypt the print job for use by the printer [column 10, lines 16-37].

As to claim 4, Slick et al teaches that the key is specific to a particular user, the method further comprising using the key to submit the print job from the client device only at the request of the particular user [column 9, lines 25-29].

As to claim 6, Slick et al teaches the method further comprising:

storing a related key on a storage device of the print server [column 8, lines 9-17].

As to claims 7 and 21, Slick et al teaches the method further comprising:

encrypting the print job with the key resulting in an encrypted print job [column 6, lines 37-49];

sending the encrypted print job from the client to the print server [column 6, lines 37-49]; and

attempting to decrypt the encrypted print job with the related key stored on the storage device of the print server [column 11, lines 36-53];

wherein, if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

As to claim 8, Slick et al teaches that installing the driver further comprises re-installing the driver with the key on the client if a driver without the key is already installed on the client [column 6, lines 22-36].

As to claim 9, Slick et al teaches that installing the driver further comprises re-configuring the driver on the client with the key if a driver without the key is already installed on the client [column 11, lines 16-35].

As to claim 10, Slick et al teaches that installing the driver with the key further comprises installing the key on the client without installing the driver if a driver configured to use the key is already installed on the client [column 6, lines 22-36].

As to claims 11 and 23, Slick et al teaches that the key allows the client to print to multiple networked printers managed by the print server [column 6, lines 8-21].

As to claims 12 and 24, Slick et al teaches that the key is provided to multiple clients [column 6 line 50 to column 7 line 4].

As to claim 19, Slick et al discloses a system for controlling a client's ability to send a print job to a printer on a network, the system comprising:

at least one client [column 10, lines 59-61];

a print server for managing distribution of print jobs to one or more printers [column 9, lines 18-47]; and

a network connecting the at least one client device, the print server and the one or more printers [column 9, lines 18-47];

wherein the print server generates a key for a specific client of the print server, the printer server then requires the specific client to use the key provided to the client when the client is submitting a print job to the print server [column 9, lines 18-47].

Slick et al does not teach embedding the key in a printer driver. Slick et al does not teach providing the key to the specific client on the network by installing the print driver on the specific client.

Imbrie et al teaches permitting encryption/decryption of data received from the intermediate device, a public key can be provided and embedded within the print driver for use with a later generated private key to encrypt or decrypt data pockets transmitted from the printing assembly 40 [0037].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Slick et al so that the key pair would have been embedded in a print driver and the keys would have been provided to the client when the driver was installed on the specific client.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Slick et al by the teaching of Imbrie et al because it provides a secure manner in which keys are distributed with differing peripheral devices [0007].

As to claim 20, Slick et al teaches that the print server is configured to:

generate the key with a utility [column 6 line 50 to column 7 line 4]; and

store a related key on a storage device [column 6 line 50 to column 7 line 4].

As to claim 22, Slick et al teaches that if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 12, lines 1-23].

As to claim 25, Slick et al teaches that the key allows any user to cause the client to send the print job to the print server [column 9, lines 18-47].

As to claim 26, Slick et al teaches that the at least one client comprises a personal computer [column 5, lines 35-45].

As to claim 27, Slick et al teaches that the configuration utility is an embedded web server that resides on the print server [column 9, lines 18-47].

As to claim 28, Slick et al teaches that the storage device is incorporated into the print server [column 9, lines 18-47].

As to claim 29, Slick et al teaches that the storage device is connected to the network, but separate from the print server [column 9, lines 18-47].

(10) Response to Argument

A. On page 10, regarding claim 13, the Appellant argues that Slick does not teach or suggest the claimed method in which a client is to be provided with a key "specifically configured for [a particular] user" and where the client will refuse to submit a print job for that particular user unless the key associated with that particular user has been provided to the client.

The examiner respectfully disagrees. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its

way to printer 20 [column 6, lines 37-49]. As seen in FIG. 4A, user-specific private key 54 is provided to encryption algorithm 65 along with printer public key 25 to generate encrypted printer public key 67, which is then stored in registry 41 under user1 entry 42 in subentry 44. As discussed above, user-specific private key 54 is preferably accessed through operating system 40 based on login id 45 for user1. In this manner, printer public key 25 is securely stored in registry 41 in an encrypted fashion for subsequent use to authenticate a stored version of printer public key 25 before using printer public key 25 to encrypt print data. As seen in FIG. 5A, user-specific public key 53 is accessed, preferably through operating system 40 [column 8, lines 49-53. User-specific public key 53 is provided to decryption algorithm 76 along with encrypted printer public key 67 to obtain decrypted printer public key 75. Printer public key 25 is retrieved from storage area 62, or if computer 10 is a networked environment as depicted in FIG. 2, printer public key 25 can be retrieved from fixed disk 31 of server 30 [column 9, lines 25-33]. As seen from the quoted text, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

B. On page 12, regarding claim 30, the Appellant argues that Slick does not teach or suggest the claimed method in which "said client will refuse to submit a print job to said printer for a particular user unless said key associated with that user has been provided to said client".

The examiner respectfully disagrees. As discussed above, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

C. On page 13, regarding claim 38, the Appellant argues that Slick only teaches the user of user-specific keys for securing other keys. The Appellant argues that Slick does not teach or suggest a system as recited with means for providing a key to a client that is specific to a user of that client and is used to encrypt print jobs from that client to a printer.

The examiner respectfully disagrees. As discussed above, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

D. On page 14, regarding claims 6 and 15, the Appellant argues that Slick does not teach or suggest that the related key is stored "on a storage device of said print server".

The examiner respectfully disagrees. Slick discloses that server 30 is used to store public keys for use by computer 10 [column 6, lines 19-21].

E. On page 15, regarding claim 1, the Appellant argues that Slick does not teach or suggest "generating a key for a specific client of the print server". The Appellant argues that Slick merely recites one printer public key that is provided to all authorized users of the printer with which to encrypt print data being sent to the printer. The Appellant argues that this teaches away from "generating a key for a specific client of the print server".

The examiner respectfully disagrees. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and

decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20 [column 6, lines 37-49]. As seen in FIG. 4A, user-specific private key 54 is provided to encryption algorithm 65 along with printer public key 25 to generate encrypted printer public key 67, which is then stored in registry 41 under user1 entry 42 in subentry 44. As discussed above, user-specific private key 54 is preferably accessed through operating system 40 based on login id 45 for user1. In this manner, printer public key 25 is securely stored in registry 41 in an encrypted fashion for subsequent use to authenticate a stored version of printer public key 25 before using printer public key 25 to encrypt print data. As seen in FIG. 5A, user-specific public key 53 is accessed, preferably through operating system 40 [column 8, lines 49-53. User-specific public key 53 is provided to decryption algorithm 76 along with encrypted printer public key 67 to obtain decrypted printer public key 75. Printer public key 25 is retrieved from storage area 62, or if computer 10 is a networked environment as depicted in FIG. 2, printer public key 25 can be retrieved from fixed disk 31 of server 30 [column 9, lines 25-33]. As seen from the

quoted text, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

F. On page 15, regarding claim 1, the Appellant argues that Slick does not teach or suggest that "generating a key for a specific client of the print server" is performed "with a print server".

The examiner respectfully disagrees. Slick discloses generating generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be

intercepted on its way to printer 20 [column 6, lines 37-49]. As seen in FIG. 4A, user-specific private key 54 is provided to encryption algorithm 65 along with printer public key 25 to generate encrypted printer public key 67, which is then stored in registry 41 under user1 entry 42 in subentry 44. As discussed above, user-specific private key 54 is preferably accessed through operating system 40 based on login id 45 for user1. In this manner, printer public key 25 is securely stored in registry 41 in an encrypted fashion for subsequent use to authenticate a stored version of printer public key 25 before using printer public key 25 to encrypt print data. As seen in FIG. 5A, user-specific public key 53 is accessed, preferably through operating system 40 [column 8, lines 49-53. User-specific public key 53 is provided to decryption algorithm 76 along with encrypted printer public key 67 to obtain decrypted printer public key 75. Printer public key 25 is retrieved from storage area 62, or if computer 10 is a networked environment as depicted in FIG. 2, printer public key 25 can be retrieved from fixed disk 31 of server 30 [column 9, lines 25-33]. As seen from the quoted text, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

G. On page 16, regarding claim 1, the Appellant argues that Imbrie fails to teach or suggest "with a print server, generating a key for a specific client of said print server".

The examiner respectfully disagrees. Imbrie was not used to teach this feature. As discussed above, Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key

pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20 [column 6, lines 37-49].

H. On page 16, regarding claim 1, the Appellant argues the combination of Slick and Imbrie fails to teach or suggest "embedding said key in a printer driver; providing said key to said specific client on said network by installing said printer driver on said specific client".

The examiner respectfully disagrees. Imbrie discloses embedding a key within a print driver [0037]. The user specific key would have been provided to the client computer when the printer driver was installed on the computer.

I. On page 16, regarding claim 1, the Appellant argues the combination of Slick and Imbrie further fails to teach or suggest that a key embedded in a printer driver "is used to submit a print job from said client to a printer on said network".

The examiner respectfully disagrees. Slick modified by the Imbrie reference teaches embedding a key in a printer driver. Figure 3 of Slick discloses generating encrypted print data to be sent to printer 20.

J. On page 17, regarding claim 1, the Appellant argues that Slick and Imbrie, did not include the claimed subject matter, particularly a method that includes, "with a print server, generating a key for a specific client of said print server, embedding said key in a printer driver on said specific client, wherein said key is used to submit a print job from said client to a printer on said network".

The examiner respectfully disagrees. As discussed above, Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a

secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20 [column 6, lines 37-49]. Slick modified by the Imbrie reference teaches embedding a key in a printer driver. Figure 3 of Slick discloses generating encrypted print data to be sent to printer 20.

K. On page 18, regarding claim 19, the Appellant argues that the combination of Slick and Imbrie does not teach or suggest the claimed print server that "generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client".

The examiner respectfully disagrees. As discussed above, Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be

installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20 [column 6, lines 37-49]. Imbrie discloses embedding a key within a print driver [0037]. The user specific key would have been provided to the client computer when the printer driver was installed on the computer.

L. On page 18, regarding claim 19, the Appellant argues that claim 19 further recites that the "print server" as opposed to some other constituent of the system, "requires said specific client to use said key provided to said client when said client is submitting a print job to said print server". The Appellant argues that all this subject matter is clearly outside the scope and content of the cited prior art.

The examiner respectfully disagrees. Slick discloses securely storing a printer public key for encryption of print data in a computing device by using a user-specific key pair which is securely stored in the computing device [column 3, lines 32-35]. As seen in FIG. 4A, user-specific private key 54 is provided to encryption algorithm 65 along with printer public key 25 to generate encrypted printer public key 67, which is then stored in registry 41 under user1 entry 42

in subentry 44. As discussed above, user-specific private key 54 is preferably accessed through operating system 40 based on login id 45 for user1. In this manner, printer public key 25 is securely stored in registry 41 in an encrypted fashion for subsequent use to authenticate a stored version of printer public key 25 before using printer public key 25 to encrypt print data. As seen in FIG. 5A, user-specific public key 53 is accessed, preferably through operating system 40 [column 8, lines 49-53. User-specific public key 53 is provided to decryption algorithm 76 along with encrypted printer public key 67 to obtain decrypted printer public key 75. Printer public key 25 is retrieved from storage area 62, or if computer 10 is a networked environment as depicted in FIG. 2, printer public key 25 can be retrieved from fixed disk 31 of server 30 [column 9, lines 25-33]. As seen from the quoted text, a user will not be able to submit print data (i.e. encrypted print data) to the printer without possession of the user-specific keys. Without the user specific keys, a user will not be able to decrypt the printer public key and submit print jobs.

M. On page 19, regarding claim 19, the Appellant argues that Slick and Imbrie did not include the claimed subject matter, particularly a system in which a "print server generates a key for a specific client of said print server, embeds said key in a printer driver; and installs said printer driver on said specific client, said printer server then requires said specific client to use said key provided to said client when said client is submitting a print job to said print server".

The examiner respectfully disagrees. As discussed above, Slick discloses generating generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user [column 6, lines 59-62]. Slick discloses that the Microsoft CAPI generates a user-specific key pair for each user of computer 10 and stores each user-specific key pair in a registry entry for the particular corresponding user

[column 6, lines 59-62]. Slick discloses that printer 20 includes a printer key pair 22 which is comprised of printer public key 25 and printer private key 23. Keys 25 and 23 are cryptographic keys which are used for encryption and decryption, respectively, of print data. Printer public key 25 is created and maintained by the manufacturer of printer 20 or can be installed on printer 20 by a system administrator [column 6, lines 26-36]. Printer public key 25 is made accessible to the public for use in the encryption of print data to send to printer 20 in a secure, encrypted manner. Printer private key 23 is also a cryptographic key which corresponds to printer public key 25, and is also created by the creator of printer public key 25. However, unlike printer public key 25, printer private key 23 is maintained under strict security within printer 20 and cannot be accessed and/or removed from printer 20. In this manner, only printer 20 has access to both of keys 23 and 25 of printer key pair 22, thereby allowing users of printer 20 to trust that encrypted print data sent to printer 20 cannot be decrypted by any unauthorized party if the encrypted print data should be intercepted on its way to printer 20 [column 6, lines 37-49]. Imbrie discloses embedding a key within a print driver [0037]. The user specific key would have been provided to the client computer when the printer driver was installed on the computer. Figure 3 of Slick discloses generating encrypted print data to be sent to printer 20.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Aravind K Moorthy/

Examiner, Art Unit 2431

Conferees:

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431